

CRYPTOGRAPHIC METHOD USING DUAL ENCRYPTION KEYS AND A WIRELESS LOCAL AREA NETWORK (LAN) SYSTEM THEREFOR

BACKGROUND OF THE INVENTION

1. Field of the Invention

[0001] The present invention relates to a wireless Local Area Network (LAN) system. More particularly, the present invention relates to a cryptographic method using dual encryption keys and a wireless Local Area Network (LAN) system therefor that is capable of increasing security by encoding data using dual encryption keys consisting of first and second group keys in an ad-hoc network.

2. Description of the Related Art

[0002] Generally, a wireless Local Area Network (LAN) system includes an ad-hoc network where a plurality of terminals, each of which includes a wireless Network Interface Card (NIC), are connected to each other and independently to wired LANs, and an infrastructure network where wireless terminals are connected to wired LANs through wireless access nodes having a wireless NIC. An ad-hoc network consists of two or more wireless terminals. Contrary to the infrastructure network, the ad-hoc network does not have a fixed wireless access node for accessing other wireless terminals.

If the respective wireless terminals of an ad-hoc network exist within a distance that allows communication between the terminals, the respective wireless terminals are recognized by each other as belonging to the same ad-hoc group by setting the same service set identifiers (SSIDs). If one wireless terminal is connected to the Internet, that wireless terminal is used as a server and the other wireless terminals within the same ad-hoc group share access to the Internet through that server using any sharing program of the Internet or any sharing menu of Microsoft Windows®.

[0003] Generally, an ad-hoc network is formed by specific users having a common interest. Since most information in the ad-hoc group is intended to be private, and that information is temporarily generated for specific purposes, the information does not have continuity. In addition, in an ad-hoc network, the creator of a group becomes a temporary group master and participants of the group are allowed participation permission in the group with only minimal information.

[0004] In a wireless LAN system of an ad-hoc network, transmission data is encoded, for communication security, to provide confidentiality and integrity of data. Due to the characteristics of an ad-hoc network, a cryptographic

method using symmetric keys is primarily used. FIG. 1 illustrates a schematic view of a conventional cryptographic method in a wireless LAN system of an ad-hoc network.

[0005] As shown in FIG. 1, in a system using symmetric keys, all wireless terminals 11, 13, 15, 17, and 19, which constitute an ad-hoc network 10, share a group key value, wherein the group key value is set by the users. That is, all users in the ad-hoc group must know the group key value in advance of transmitting data, which causes some inconvenience. Further, although the users know the group key value in advance, the group key value must often be modified to minimize exposure of the group key value to hacking by a malicious user. Therefore, the group key value must be frequently created, distributed, and modified. However, since no apparatus provides such a function in a current ad-hoc network, the high possibility of being hacked by a malicious user poses a serious threat.

SUMMARY OF THE INVENTION

[0006] The present invention provides a cryptographic method in a wireless local area network (LAN) system of an ad-hoc network using dual encryption keys that is capable of confirming data security by creating a first group key

using a group password, and then by creating, distributing, and modifying a second group key for use upon data transmission in a wireless terminal functioning as a key distribution center, using a random key generation algorithm.

[0007] The present invention also provides a wireless LAN system that is capable of strengthening security by encoding data using dual encryption keys consisting of a first and second group keys.

[0008] According to a feature of the present invention, there is provided a cryptographic method using dual keys in a wireless local area network (LAN) system, including (a) generating a first group key in N wireless terminals forming an ad-hoc group, where N is equal to or greater than two; (b) generating a second group key in a main wireless terminal to perform a key distribution center function among the N wireless terminals, and transmitting the second group key to (N-1) sub wireless terminals; and (c) encoding data using the second group key, and transmitting the encoded data between the N wireless terminals.

[0009] Preferably, when the main wireless terminal is withdrawn from the ad-hoc group, the main wireless terminal transfers a function of key

distribution center to a sub wireless terminal selected from among the (N-1) sub wireless terminals, so that the sub wireless terminal acts as the main wireless terminal.

[0010] The cryptographic method may further include modifying the second group key in the main wireless terminal according to a predetermined modification time period, and transmitting the modified second group key to the (N-1) sub wireless terminals.

[0011] According to another feature of the present invention, there is provided a computer readable medium having embodied thereon a computer program for the above cryptographic method using the dual encryption keys in a wireless LAN system.

[0012] According to still another feature of the present invention, there is provided a wireless local area network (LAN) system comprising: N, where N is equal to or greater than two, wireless terminals which form an ad-hoc group, and create a first group key, wherein the N wireless terminals include: a main wireless terminal for performing a key distribution center function in the ad-hoc group, for creating a second group key and encoding data using the second group key, and for transmitting the encoded data between the

remaining wireless terminals; and (N-1) sub wireless terminals for receiving the second group key from the main wireless terminal and encoding data using the second group key, and for transmitting the encoded data between the remaining wireless terminals.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] The above and other features and advantages of the present invention will become more apparent to those of ordinary skill in the art by describing in detail preferred and exemplary embodiments thereof with reference to the attached drawings in which:

[0014] FIG. 1 illustrates a schematic view of a conventional cryptographic method in a wireless local area network (LAN) system of an ad-hoc network;

[0015] FIG. 2 is a flow chart illustrating a cryptographic method using dual encryption keys in a wireless LAN system of an ad-hoc network, according to a preferred embodiment of the present invention;

[0016] FIG. 3 is a flow chart illustrating a method of modifying a second group key, according to an embodiment of the present invention;

[0017] FIG. 4 is a block diagram showing a wireless LAN system of an ad-hoc network, according to a preferred embodiment of the present invention; and

[0018] FIG. 5 illustrates a schematic view of the operational relationships of the components of FIG. 4.

DETAILED DESCRIPTION OF THE INVENTION

[0019] Korean Patent Application No. 2002-39156, filed on July 6, 2002, and entitled: "Cryptographic Method Using Dual Encryption Keys and Wireless Local Area Network (LAN) System Therefor," is incorporated by reference herein in its entirety.

[0020] The present invention will now be described more fully hereinafter with reference to the accompanying drawings, in which preferred and exemplary embodiments of the invention are shown. The invention may, however, be embodied in different forms and should not be construed as limited to the embodiments set forth herein. Rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art.

[0021] FIG. 2 is a flow chart illustrating a cryptographic method using dual encryption keys in a wireless LAN system of an ad-hoc network, according to a preferred embodiment of the present invention. The present cryptographic method includes, in step 21, setting a main wireless terminal, in step 22, creating a first group key, in step 23, creating a second group key, in step 24, transmitting the second group key, and, in step 25, transmitting data.

[0022] Referring to FIG. 2, in step 21, among N (where N is preferably an integer equal to or greater than two) wireless terminals forming an ad-hoc group, a main wireless terminal functions as a key distribution center (KDC). Initially, the creator of the ad-hoc group is set as the main wireless terminal in order to function as the key distribution center. When the main wireless terminal is withdrawn from the ad-hoc group, the main wireless terminal is able to transfer the function of key distribution center to another wireless terminal selected from among the (N-1) wireless terminals remaining in the ad-hoc group.

[0023] Successively, in step 22, a first group key (LSK) is created using a group password in the N wireless terminals. Then, in step 23, a second

group key (SSK1) is created in the main wireless terminal for use in transmitting data between wireless terminals. The process of creating the second group key (SSK1) in step 23 will now be described in greater detail. After the creation of the first group key in step 22, in step 23a, a second group key request message from respective wireless terminals is encoded with the first group key and is transmitted to the main wireless terminal. In step 23b, the second group key request message is decoded in the main wireless terminal using the first group key. Then, in step 23c, a second group key (SSK1) is created in the main wireless terminal, according to the decoded message. In the above process, the first and second group keys may be created using a general key generation algorithm.

[0024] Subsequently, in step 24, the second group key (SSK1), which was created in the main wireless terminal, is encoded with the first group key and is transmitted to the (N-1) wireless terminals in the ad-hoc network. Then, in step 25, data is encoded using the second group key and is transmitted between the N wireless terminals.

[0025] FIG. 3 is a flow chart illustrating a method of modifying a second group key, according to an embodiment of the present invention. First, if a

modification time period is predetermined in the main wireless terminal, in step 31, a second group key (SSK1) is modified according to the predetermined modification time period. This second group key modification may be performed using a general key generation algorithm, as in step 23 of FIG. 2. Then, in step 32, the modified second group key (SSK2), which was modified in the main wireless terminal, is encoded using the non-modified second group key (SSK1), and is transmitted to the (N-1) wireless terminals in the ad-hoc network. The modified second group key (SSK2) transmitted from the main wireless terminal is then decoded using the non-modified second group key (SSK1), so that, in step 33, the decoded modified second group key (SSK2) can be used as the encryption key in transmitting data between respective wireless terminals.

[0026] By modifying a second group key according to a predetermined modification time period, a second group key generated from a main wireless terminal is used only during a predetermined time period, and is discarded after the time period expires. This is intended to limit the ability of a would-be hacker to analyze passwords or to detect the second group keys stored in each wireless terminal.

[0027] FIG. 4 is a block diagram showing a wireless LAN system of an ad-hoc network, according to an embodiment of the present invention. One ad-hoc group includes N wireless terminals, generally including, a main wireless terminal 45, which functions as a key distribution center, and (N-1) sub wireless terminals 41, wherein N is preferably an integer equal to or greater than two.

[0028] The sub wireless terminal 41 includes a first group key generator 42, a first encryption unit 43, and a first key management unit 44. The main wireless terminal 45 includes a second group key generator 46, a second encryption unit 47, and a second key management unit 48. Initially, a main wireless terminal 45 is set as the creator of an ad-hoc group. However, when the main wireless terminal 45 is withdrawn from the ad-hoc group, the main wireless terminal 45 is able to transfer the function of key distribution center to another wireless terminal selected from among the (N-1) wireless terminals remaining in the ad-hoc group. Accordingly, each of the remaining wireless terminals 41 constituting the ad-hoc group, as well as the original main wireless terminal 45, must have the ability to function as a key distribution center.

[0029] Now, operations of the wireless LAN system of the ad-hoc network will be described sequentially in connection with FIG. 5. FIG. 5 illustrates a schematic view of the operational relationships of the components of FIG. 4.

[0030] With reference to FIGS. 4 and 5, a first group key generator 42 of a sub wireless terminal 41 creates a first group key (LSK) 412 using a group password 411 input from a user, and outputs the first group key (LSK) 412 to a first encryption unit 43. Similarly, a second group key generator 46 of a main wireless terminal 45 creates a first group key (LSK) 452 using a group password 451 input from a user, and outputs the first group key (LSK) 452 to a second encryption unit 47. The first group keys (LSK) 412 and 452 can be created using a general key generation algorithm.

[0031] If a first key management unit 44 recognizes that the first group key (LSK) 412 has been created in the first group key generator 42, the first key management unit 44 generates a second group key (SSK1) request message 413. The generated second group key (SSK1) request message 413 is supplied to the first encryption unit 43.

[0032] The first encryption unit 43 stores the first group key (LSK) 412 supplied from the first group key generator 42, receives the second group

key (SSK1) request message 413 generated from the first key management unit 44, encodes the second group key (SSK1) request message 413 using the stored first group key (LSK) 412, and transmits the encoded result to the second encryption unit 47 of the main wireless terminal 45 through a wireless channel WC.

[0033] In FIGS. 4 and 5, reference numeral 413 represents any one of a series of messages communicated between the first key management unit 44 and the first encryption unit 43. Reference numeral 414 represents any one of a series of group keys communicated to the first encryption unit 43 from the first key management unit 44. Similarly, reference numeral 453 represents any one of a series of messages communicated between the second key management unit 48 and the second encryption unit 47. Reference numeral 454 represents any one of a series of group keys communicated to the second encryption unit 47 from the second key management unit 48.

[0034] In the main wireless terminal 45, the second encryption unit 47 stores the first group key (LSK) 452 supplied from the second group key generator 46, decodes the encoded second group key (SSK1) request message

transmitted from the sub wireless terminal 41 using the first group key (LSK) 452, and transmits the decoded message 453 to the second key management unit 48.

[0035] The second key management unit 48 receives the second group key request (SSK1) message 453 decoded by the second encryption unit 47, creates a second group key (SSK1), and supplies a second group key (SSK1) response message 453, which includes the created second group key (SSK1) 454, to the second encryption unit 47. The second group key (SSK1) 454 may also be created using a general random key generation algorithm. The second encryption unit 47 encodes the second group key (SSK1) response message 453 using the first group key (LSK) 452 and transmits the encoded result to the first encryption unit 43 through a wireless channel WC.

[0036] In the sub wireless terminal 41, the first encryption unit 43 decodes the encoded second group key (SSK1) response message, transmitted from the main wireless terminal 45, using the first group key (LSK) 412 and transmits the decoded message 413 to the first key management unit 44. The first key management unit 44 extracts the second group key (SSK1) 414

from the decoded message 413 and supplies the extracted second group key (SSK1) 414 to the first encryption unit 43. The first encryption unit 43 encodes data 415 input from a user, using the second group key (SSK1) 414, and transmits the encoded result. Similarly, in the main wireless terminal 45, the second encryption unit 47 encodes data 455 input from a user, using the second group key (SSK1) 454, and transmits the encoded result.

[0037] The second key management unit 48 of the main wireless terminal 45 predetermines a constant modification time period, creates a modified second group key (SSK2), which is modified according to the predetermined modification time period, using a random key generation algorithm, and supplies a second group key (SSK2) modification message 453, which includes the modified second group key (SSK2) 454, to the second encryption unit 47. The second encryption unit 47 encodes the second group key (SSK2) modification message 453, using the non-modified second group key (SSK1), and transmits the encoded result to the first encryption unit 43 through a wireless channel WC.

[0038] The first encryption unit 43 decodes the encoded second group key (SSK2) modification message, using the non-modified second group key

(SSK1), and supplies the decoded message 413 to the first key management unit 44. The first key management unit 44 extracts the modified second group key (SSK2) from the decoded second group key (SSK2) modification message 413, and supplies the extracted second group key (SSK2) 414 to the first encryption unit 43. The first encryption unit 43 encodes data 415 input from a user, using the second group key (SSK2) 414, and transmits the encoded result. Similarly, in the main wireless terminal 45, the second encryption unit 47 encodes data 455 input from a user, using the second group key (SSK2) 454, and transmits the encoded result.

[0039] The above-described preferred and exemplary embodiments of the present invention may be embodied as computer programs and may also be embodied in a general-purpose digital computer for executing the computer programs using a computer readable medium. The computer readable medium may include storage media, such as magnetic storage media (e.g., ROMs, floppy discs, hard discs, etc.), optically readable media (e.g., CD-ROMs, DVDs, etc.), and carrier waves (transmissions over the Internet).

[0040] As described above, according to the preferred and exemplary embodiments of the present invention, it is possible to increase users'

convenience in a wireless LAN system of an ad-hoc network by easily creating a first group key using a group password. Further, the inconvenience regarding key management in a symmetric-key algorithm can be overcome by using a random key generation algorithm to create, distribute, and modify a second group key for use upon data transmission in a wireless terminal functioning as a key distribution center.

[0041] In addition, since the first group key has a low frequency of use and the second group key is modified at predetermined time intervals, the chance of an unwanted decryption by a malicious user is reduced, thereby increasing and verifying data security within a group.

[0042] In addition, it is possible to continuously perform key management, i.e., creation, distribution, and modification of a second group key, by allowing the wireless terminal that is the creator of the ad-hoc group to function as a key distribution center and to transfer that function of key distribution center to another wireless terminal when the wireless terminal that has functioned as the key distribution center is withdrawn from the ad-hoc network.

[0043] Preferred and exemplary embodiments of the present invention have been disclosed herein and, although specific terms are employed, they are used and are to be interpreted in a generic and descriptive sense only and not for purpose of limitation. Accordingly, it will be understood by those of ordinary skill in the art that various changes in form and details may be made without departing from the spirit and scope of the present invention as set forth in the following claims.